BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-210

1 MAY 1996
Communications

★*CRYPTOGRAPHIC ACCESS*

NOTICE: This publication is available digitally. Contact your Publishing Distribution Office (PDO) for the monthly CD-ROM or access to the bulletin board system. The target date for discontinuing paper publications is December, 1996.

This Air Force instruction (AFI) implements Department of Defense Directive DoDD 5205.8, *Access to Classified Cryptographic Information*, February 20, 1991. It establishes the Air Force Cryptographic Access Program (CAP) and provides guidelines and procedures to grant access to classified cryptographic information the DoD produces, owns, or controls. Refer to AFKAG-1, *Air Force Communications Security (COMSEC) Operations*, for general guidance on handling, accountability, storage, transportation, inspection, and destruction of COMSEC material. See Attachment 1 for a glossary of references, abbreviations, acronyms, and terms. Major commands (MAJCOM), field operating agencies, and direct reporting units may supplement this instruction only by coordinating with Headquarters Air Force Command, Control, Communications, and Computer Agency, Systems Security Support and Development Branch (HQ AFC4A/SYS), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5233. Send one copy of final supplement to HQ AFC4A, Policy Branch (HQ AFC4A/XPXP), 203 West Losey Street, Room 1065, Scott AFB IL 62225-5233. Send recommended changes or comments to HQ AFC4A/SYS, through appropriate channels, using AF Form 847, **Recommendation for Change of Publications**. Send an information copy to HQ USAF, Information Warfare Division (HQ USAF/SCTW), 1250 Air Force Pentagon, Washington DC 20330-1250. Refer conflicts between this AFI and other Air Force publications to HQ AFC4A/XPXP, 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5224. This instruction directs collecting and maintaining information subject to the Privacy Act of 1974 authorized by Title 10 United States Code (U.S.C.), Section 8013, *Secretary of the Air Force, Powers and Duties.* Systems of Record F030 AF A, applies.

SUMMARY OF REVISIONS

This revision corrects attachment 2 and adds attachment 3.

1. General. Personnel occupying the following positions, which require continuing access to cryptographic information, must consent to the requirements of the CAP before getting access to cryptographic material:

1.1. Personnel assigned to COMSEC accounts. *EXCEPTION*: COMSEC personnel assigned to administrative MAJCOM accounts do not require access.

1.2. Personnel with access to **TOP SECRET** cryptographic media.

1.3. Personnel who operate key-generating equipment (for example, KG-83).

1.4. Personnel who operate certification authority workstations.

1.5. Personnel who prepare, authenticate, or decode nuclear control orders (valid or exercise).

1.6. Personnel assigned to secure communications facilities whose duties require keying of five or more different types of cryptographic equipment (that is, KG-84, KY-57, KY-65, KG-94, KG-194).

1.7. Personnel who perform duties as cryptographic maintenance, engineering, or installation technicians.

1.8. Personnel who receive, stock, store, package, and ship COMSEC material for COMSEC accounts 616600, 640000, and 670000.

2. Responsibilities.

2.1. COMSEC Managers. Oversee the CAP and provide written local procedures, as required, to all COMSEC responsible officers (CRO) of personnel identified in paragraph 1.

Supersedes: AFI 33-210, 1 April 1996.
OPR: HQ AFC4A/SYS (CMSgt James R. Hogan)
Certified by: HQ USAF/SCXX (Lt Col G. L. Fiedler)
Pages: 7/Distribution: F

2.2. Unit Commanders. Appoint, in writing, a CAP administrator to grant and withdraw cryptographic access and witness signatures on AFCOMSEC Form 9, **Formal Cryptographic Access (FCA) Certificate**. HQ AFC4A does not require copies of the CAP administrator appointment letters.
2.3. The CAP Administrator. Identifies and grants cryptographic access in the commander's name to all personnel who require authorized access to classified cryptographic information.

3. Cryptographic Access Eligibility. To qualify for cryptographic access, a person must meet all of the following qualifications:
3.1. Hold U.S. citizenship.
3.2. Be a DoD civilian employee, a DoD-cleared contractor or contractor employee, or a military service member.
3.3. Require cryptographic access to perform official duties.
3.4. Have a security clearance and security investigation appropriate to the classified cryptographic information level accessed.
3.5. Receive a security briefing detailing the sensitive nature of cryptographic material and the individual's responsibility to protect cryptographic material (see Attachment 2).
3.6. Agree to report contacts with individuals of any nationality to their security manager or supervisor when illegal or unauthorized access is sought to classified or sensitive information, or there is a concern that they may be the target of exploitation by a foreign entity (see AFI 31-501, *Personnel Security Program Management).*
3.7. Consent to periodic counterintelligence security polygraph examinations and sign the AFCOMSEC Form 9 that contains both the cryptographic access certification and the polygraph consent.

4. Cryptographic Access.
4.1. For each individual granted access, the CAP administrator must follow these certification procedures:
4.1.1. Prepare an AFCOMSEC Form 9 in original and two copies. Submit the signed original to HQ AFC4A/SYS. Give one copy to the individual and one to the individual's CRO. Maintain the certificate as long as the individual requires cryptographic access at that location. Type the form accurately and completely. HQ AFC4A/SYS returns all improperly completed AFCOMSEC Forms 9. Provide the following information:
4.1.1.1. Social Security Number (SSN).
4.1.1.2. Name (include "Jr.", "Sr.", or "III" after middle initial).
4.1.1.3. Date Granted Access. Year (YY), month (Mon), day (DD) (use the date that the individual signs the AFCOMSEC Form 9).
4.1.1.4. Supporting COMSEC Account Number.
4.1.1.5. Unit and Office Symbol.
4.1.1.6. Assigned Installation (enter the base or location of permanent assignment).
4.1.1.7. Date Access Withdrawn.
4.1.1.8. Reason for Withdrawal. (See paragraph 8 for explanations.)
4.1.2. Brief personnel requiring cryptographic access at temporary duty locations before they leave the home station. Include the individual's access status on all clearance status notifications.
4.1.3. Submit cryptographic access name changes on a new AFCOMSEC Form 9, with the individual's SSN, to HQ AFC4A/SYS, or make the change on the cryptographic access verification listing.
4.2. HQ AFC4A/SYS must file the original access certificate.

5. Foreign National Contact and Foreign Travel. All personnel with cryptographic access must report to their local security manager or supervisor contacts with individuals of any nationality when illegal or unauthorized access is sought to classified or sensitive information, or there is a concern that they may be the target of exploitation by a foreign entity (see AFI 31-501).
5.1. HQ AFC4A/SYS maintains reports of contacts in the CAP database as a historical and security record.

6. Polygraph Examinations. The Air Force Office of Special Investigations (AFOSI) Regional Polygraph Offices, in conjunction with the AFOSI Investigative Operations Center (IOC), schedule and administer polygraph examinations. HQ AFC4A/SYS maintains a list of all persons who currently have cryptographic access status and periodically provide copies to regional AFOSI offices.

7. Cryptographic Access Verification Lists.
7.1. HQ AFC4A/SYS periodically sends a local list of the CAP database to each supporting COMSEC account.
7.2. CAP administrators compare this cryptographic access list to those persons currently having access to ensure an accurate database. Instructions accompany each list.
7.3. Units may request cryptographic access lists from HQ AFC4A/SYS through their supporting COMSEC manager.

8. Access Withdrawal. CAP administrators withdraw an individual's access by one of the following three methods:
8.1. Administrative Withdrawal. Applies to personnel reassigned to another base or unit, or to positions that don't require cryptographic access. Administrative withdrawal is without prejudice and is simply an acknowledgment that the need-to-know no longer exists. Enter "Administrative" on the AFCOMSEC Form 9. Messages advising administrative withdrawals from cryptographic access are not required.
8.2. Suspension. Applies to personnel who have their security clearance or other special access suspended in accordance with AFI 31-501. Withdraw these individuals from duties requiring cryptographic access until the Air Force adjudicates the case. Review suspensions every 90 days and provide updates to AFC4A/SYS. Upon adjudica-

tion, submit a new AFCOMSEC Form 9 that changes the individual's withdrawal status to administrative withdrawal or permanent revocation.

8.2.1. If an individual is suspended from access with a special security file and then separates or is discharged from the Air Force before the investigation is completed, the commander determines the individual's trustworthiness by designating the withdrawal category on AFCOMSEC Form 9 (see paragraph 8.1). Withdraw the person administratively if the individual is trustworthy.

8.2.2. The CAP administrator submits an AFCOMSEC Form 9 marked "Suspension" to HQ AFC4A/SYS, along with a letter or message stating the reason for the suspension (see Attachment 3). Stamp correspondence containing reasons for the withdrawal: **FOR OFFICIAL USE ONLY**.

8.3. Revocation. Applies to personnel who have their security clearance eligibility revoked, have their special access denied, or are permanently removed for cause. Withdraw all cryptographic access permanently or until security clearance eligibility is reinstated (see AFI 31-501).

8.3.1. The CAP administrator submits an AFCOMSEC Form 9 marked "Revocation," along with a letter or message stating the reason to HQ AFC4A/SYS (see Attachment 3).

8.3.2. The unit commander or the civilian equivalent (facility security manager) must sign AFCOMSEC Forms 9 dealing with revocations.

8.4. Access Withdrawal and Termination. CAP administrators formally terminate an individual's access by following these procedures:

8.4.1. Complete the termination section on the copy of the locally retained cryptographic access certificate and make two copies. Certificates must include the reason for the withdrawal, the date that the withdrawal took effect, and the debriefing officer's signature.

8.4.2. Maintain one copy of the completed withdrawal certificate locally for 90 days (transitory file) after the date of the withdrawal.

8.4.3. Give one copy to the individual (when person is available).

8.4.4. Submit the original withdrawal certificate to HQ AFC4A/SYS.

9. Certificates of Personnel Declining Cryptographic Access. The CAP administrator sends HQ AFC4A/SYS the original AFCOMSEC Form 9 for individuals who decline access. These certificates contain all the information on the individual except the signature. In the form's "Payroll Signature of Above Named Individual" block, enter: "Individual Refused to Accept Cryptographic Access".

10. Commander's Administrative Actions on Personnel Declining Polygraph Testing. Individuals consent to periodic polygraph examinations as a condition of having cryptographic information access when they sign the AFCOMSEC Form 9.

10.1. Commanders deny cryptographic access to personnel who will not consent to polygraph testing or who refuse to take a particular polygraph examination after giving an initial consent.

10.2. The following advisory opinion from HQ USAF/JAG, 20 April 1989, applies: "Persons denied access to cryptographic information for refusing to consent to polygraph examinations may not be assigned to positions requiring access to cryptographic information. (DoD Directive 5210.48, *DoD Polygraph Program*, December 24, 1984, paragraphs 7 and 8.) If refusal occurs after assignment, a civilian employee is reassigned to a position of equal pay and grade in the Air Force, if available, or to such a position in another DoD component. (DoD Directive 5210.48, paragraph 8.) The DoD Directive does not address what happens if no such position is available in another DoD component. In our opinion, the civilian employee must be offered positions of lesser grade or pay, if available. Otherwise, employment in Federal service is terminated. Air Force members ineligible for a cryptographic position for refusing to consent to a polygraph examination are reassigned as provided in military personnel regulations. No other adverse action may be taken concerning employees or members who refuse to consent to polygraph examinations required as a condition for access to certain cryptographic information."

10.3. DoDD 5210.48, paragraph 9, also provides for actions when a polygraph examination indicates deception. The examiner first attempts to resolve the issue in a post-examination interview. If that is unsuccessful, and the matter raises serious questions relevant to access, hold another polygraph examination.

If it does not resolve the issue, then conduct a comprehensive investigation.

10.3.1. Authorize adverse action only when this investigation discloses derogatory information that independently justifies the adverse action. However, base adverse action solely on the polygraph examination if the Secretary of the Air Force personally determines that the cryptographic information is of such extreme sensitivity that access under the circumstances poses an unacceptable risk to the national security.

10.4. Administratively withdraw persons who refuse a polygraph examination after initially consenting.

11. Prescribed Form. This instruction prescribes AFCOMSEC Form 9, **Cryptographic Access Certificate.**

JOHN S. FAIRFIELD, Lt General, USAF
DCS/Command, Control, Communications, and Computers

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

DoDD 5205.8, *Access to Classified Cryptographic Information*, February 20, 1991
DoDD 5210.48, *DoD Polygraph Program*, December 24, 1984
AFPD 33-2, C4 *Systems Security*
AFI 31-501, *Personnel Security Program Management*
AFI 33-211, *Communications Security (COMSEC) User Requirements*
AFKAG-1, *Air Force Communications Security* (COMSEC) Operations
Privacy Act of 1974
Title 10 U.S.C., Section 8013, *Secretary of the Air Force, Powers and Duties.* Systems of Record F030 AF A

Abbreviations and Acronyms

AFI−Air Force Instruction
AFOSI−Air Force Office of Special Investigations
CAP−Cryptographic Access Program
COMSEC−Communications Security
CRO−COMSEC Responsible Officer
DoD−Department of Defense
HQ AFC4A−Headquarters Air Force Command, Control, Communications,and Computer Agency
HQ USAF−Headquarters United States Air Force
IOC−Investigative Operations Center
MAJCOM−Major Command
SSN−Social Security Number

Terms

Access—The capability and opportunity to gain knowledge of or to alter information or material.
Classified Cryptographic Information—1. Cryptographic keys and authenticators classified and designated as CRYPTO. 2. Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, including depot-level maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic computer software.
Cryptographic Access Program (CAP)—A program to protect national security information and govern access to cryptographic information that the DoD produces, controls, or owns.
CAP Administrators—Individuals responsible for granting and withdrawing cryptographic access within a particular unit. Commanders appoint CAP administrators.
Inadvertent Exposure—The accidental disclosure of COMSEC information to a person who does not have authorized access.

CRYPTOGRAPHIC ACCESS BRIEFING

A2.1. You were selected to perform duties that will require access to US classified cryptographic information.
Before the Air Force grants you this access, you must understand the safeguards that protect this information, the directives that govern authorized access, and the penalties you will incur for the unauthorized disclosure, unauthorized retention, or negligent handling of United States classified cryptographic information. Failure to properly safeguard this information could cause serious to exceptionally grave damage or irreparable injury to the national security of the United States.

A2.2. United States classified cryptographic information is especially sensitive because we use it to protect classified information. You can use any particular piece of cryptographic keying material and any specific cryptographic technique to protect a large quantity of classified information during transmission.

If the integrity of a cryptographic system is breached at any point, all information protected by the system might be compromised. The safeguards placed on United States classified cryptographic information is a necessary component of government programs to make sure material vital to our national security remains secret.

A2.3. Because access to United States classified cryptographic information is granted on a strict need-to-know basis, you will only receive access to the cryptographic information necessary to perform your duties. You must become familiar with AFI 33-211, *Communications Security (COMSEC) User Requirements,*or AFKAG-1, *Air Force Communications Security (COMSEC) Operations* as appropriate.

★A2.4. Timely reporting of any known or suspected compromise of US classified cryptographic information is especially important. If a compromised cryptographic system goes unreported, our continued use of the system can result in the loss of all the information it protects. If you report the compromise, we can take steps to lessen an adversary's advantage gained through the compromise of the information.

A2.5. As a condition of access to United States classified cryptographic information, you must acknowledge the possibility that you are subject to a periodic counterintelligence-scope polygraph examination. We administer this examination according to the provisions of DoDD 5210.48 and applicable law. This polygraph examination only encompasses questions concerning disloyal activities, espionage, sabotage, terrorism, and general honesty and trustworthiness.

A2.6. You have the right to refuse to take a counterintelligence-scope polygraph examination. If you refuse, we will not take adverse action, but will deny you access to United States classified cryptographic information. If you do not want to sign the cryptographic access certificate at this time, I will terminate this briefing and the briefing administrator will record your decision on the cryptographic access certificate. Choosing not to sign the certificate has the same effect as refusing to take the exam.

A2.7. The intelligence services of some foreign governments prize the acquisition of United States classified cryptographic information. They will go to extreme lengths to compromise United States citizens and force them to divulge cryptographic techniques and materials that protect the nation's secrets around the world. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion. You must stay alert so that you can recognize and counter such attempts. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, United States classified cryptographic information. You must report any attempt, either through friendship or coercion, to solicit your knowledge regarding the United States classified cryptographic information you possess immediately to your commander or local Air Force Office of Special Investigations (AFOSI) office. You must also report any unofficial foreign travel to your local security manager so you may receive specific information concerning security issues related to your foreign travel.

A2.8. In view of these risks, you must agree to report contacts with individuals of any nationality to your security manager or supervisor when illegal or unauthorized access is sought to classified or sensitive information, or there is a concern that you may be the target of exploitation by a foreign entity.

A2.9. Finally, you must be aware that if you willfully or negligently disclose United States classified cryptographic information to any unauthorized persons, you are subject to administrative and civil sanctions, including adverse personnel actions, as well as criminal sanctions under the *Uniform Code of Military Justice* and the criminal laws of the United States.

★SAMPLE MESSAGES

A3.1. Reason for Suspension.

DATE TIME GROUP

FM 123SQ ANYWHERE AFB TX//CA654321//

TO HQ AFC4A SCOTT AFB IL//SYSC//

UNCLAS E F T O FOUO

SUBJ: CHANGE IN CRYPTOGRAPHIC ACCESS STATUS

1. THE CRYPTOGRAPHIC ACCESS FOR JOHN Q. DOE, SSN 123-45-6789, WAS SUSPENDED DUE TO *(State Reason for Suspension).*

2. AFCOMSEC FORM 9 MAILED 22 OCT 92.

3. POC IS MSGT MANAGER OR SGT ACCOUNTANT, DSN 555-1234.

A3.2. 90-Day Update for Suspension.

DATE TIME GROUP

FM 123SQ ANYWHERE AFB TX//CA654321//

TO HQ AFC4A SCOTT AFB IL//SYSC//

UNCLAS E F T O FOUO

SUBJ: CHANGE IN CRYPTOGRAPHIC ACCESS STATUS

1. THIS IS THE FIRST 90 DAY STATUS UPDATE ON THE SUSPENSION OF JOHN Q. DOE, SSN 123-45-6789. INDIVIDUAL IS (STATE PENDING ACTION OR NO CHANGE IN STATUS).

2. POC IS MSGT MANAGER OR SGT ACCOUNTANT, DSN 555-1234.

A3.3. Reason for Revocation.

DATE TIME GROUP

FM 123SQ ANYWHERE AFB TX//CA654321//

TO HQ AFC4A SCOTT AFB IL//SYSC//

UNCLAS E F T O FOUO

SUBJ: CHANGE IN CRYPTOGRAPHIC ACCESS STATUS

1. THE CRYPTOGRAPHIC ACCESS FOR JOHN Q. DOE, SSN 123-45-6789, WAS REVOKED DUE TO (STATE REASON FOR REVOCATION).

2. AFCOMSEC FORM 9, SIGNED BY THE COMMANDER, MAILED 15 DEC 92.

3. POC IS MAJ COMMANDER, DSN 555-1234.